

## MODIFIED LU-LEE CRYPTOSYSTEM

*Indexing terms: Codes, Information theory*

A modified Lu-Lee cryptosystem is proposed which appears to be resistant to the cryptanalytic attacks on the original Lu-Lee scheme. The data expansion due to encryption is moderate, and the size of the public key is also quite small.

**Introduction:** We begin with the basic principles of the Lu-Lee cryptosystem.<sup>1</sup> Let  $r = p_1 p_2$  be a number around 320 bits long, with  $p_1, p_2$  each around 160 bits long.  $a_{ij}, i, j = 1, 2$ , are four numbers, each around 16 bits long, satisfying  $a_{11}a_{22} - a_{12}a_{21} \neq 0$ . Let  $C_j = a_{ij} \pmod{p_i}, i = 1, 2, j = 1, 2$ . The messages to be encrypted consist of pairs of numbers  $(m_1, m_2)$  satisfying the condition  $a_{11}m_1 + a_{12}m_2 < p_1$  for  $i = 1, 2$ . The public encryption key consists of  $(r, C_1, C_2)$  and the bounds  $M_1$  and  $M_2$  on  $m_1$  and  $m_2$ , respectively, whereas the secret decryption key consists of the parameters  $(p_1, p_2, a_{11}, a_{12}, a_{21}, a_{22})$ .

A message  $(m_1, m_2)$  is encrypted as

$$x \equiv C_1 m_1 + C_2 m_2 \pmod{r}$$

Decryption is performed as follows. First, the residues

$$x_i \equiv x \pmod{p_i} \quad i = 1, 2$$

are computed. Then the pair  $(m_1, m_2)$  is determined by solving the two linear equations

$$a_{11}m_1 + a_{12}m_2 = x_i \quad i = 1, 2$$

which, by the condition imposed above, have the original message as the solution.

Algorithms have been devised<sup>2,3</sup> which enable a cryptanalyst to obtain  $(m_1, m_2)$  without a knowledge of  $p_1, p_2$ . The fact that to every cryptogram there corresponds a unique message is the basis of these schemes. Another attack<sup>4</sup> uses the fact that  $C_i, i = 1, 2$ , have small residues  $a_{ij}$  modulo the unknown factors, and succeeds in finding  $p_1, p_2$  and hence  $a_{ij}$ . In the following Section we propose a modification of the Lu-Lee scheme which appears resistant to both these types of attack.

**Modified Lu-Lee cryptosystem:** As in the Lu-Lee scheme, the secret decryption key is a set of numbers  $(p_1, p_2, a_{ij}, i = 1, 2, j = 1, 2)$  and the encryption key is the set  $(r, C_1, C_2)$ . The  $a_{ij}$  satisfy

- (a)  $a_{12} > a_{22}$
- (b)  $a_{21} > a_{11}$
- (c) the  $a_{ij}, i = 1, 2, j = 1, 2$  are at least 200 bits long.

Furthermore, the numbers  $r, p_1, p_2$  are chosen such that  $\text{limit } M_1 = \text{limit } M_2 = 2^{50}$ . Thus one possible choice may fix  $p_1$  and  $p_2$  at 252 bits each, and thus  $r$  at 504 bits.

**Encryption:** Message encryption is performed in the following manner:

- (1) Represent the message  $m$  as an integer less than  $2^{199}$ .
- (2) Randomly choose a pair of integers  $(m_1, m_2)$  with  $m_i < M_i, i = 1, 2$ , and compute  $m_e = m + C_1 m_1 + C_2 m_2 \pmod{r}$  as the encrypted message.

$$\begin{aligned} m_e &= C_1 m_1 + C_2 m_2 + m \pmod{r} \\ &= \{(C_1 m_1 + C_2 m_2) \pmod{r} + m \pmod{r}\} \pmod{r} \\ &= (x_e + m) \pmod{r} \end{aligned}$$

Similarly

$$\begin{aligned} m'_e &= (x'_e + m') \pmod{r} \\ m_e \pmod{p_1} &= \{x_e \pmod{p_1} + m \pmod{p_1}\} \pmod{p_1} \\ &= x_1 + m \pmod{p_1} \end{aligned}$$

Similarly

$$m_e \pmod{p_2} = x_2 + m \pmod{p_2}$$

and

$$m'_e \pmod{p_i} = x'_i + m' \pmod{p_i} \quad i = 1, 2$$

$m_e = m'_e$  implies that

$$x_1 - x'_1 = x_2 - x'_2 = m - m' \quad (2)$$

since  $m, m', x_i, x'_i < p_i, i = 1, 2$ . Furthermore,  $|(m - m')|$  is less than  $a_{ij}, i = 1, 2, j = 1, 2$ . However, by definition

$$\begin{aligned} x_1 &= a_{11}m_1 + a_{12}m_2 \\ x_2 &= a_{21}m_1 + a_{22}m_2 \end{aligned} \quad (3)$$

and

$$\begin{aligned} x'_1 &= a_{11}m'_1 + a_{12}m'_2 \\ x'_2 &= a_{21}m'_1 + a_{22}m'_2 \end{aligned} \quad (4)$$

Therefore, from eqns. 2, 3 and 4 we obtain

$$\begin{aligned} a_{11}(m_1 - m'_1) + a_{12}(m_2 - m'_2) &= a_{21}(m_1 - m'_1) \\ &+ a_{22}(m_2 - m'_2) \end{aligned}$$

Therefore

$$(a_{11} - a_{21})(m_1 - m'_1) = (a_{22} - a_{12})(m_2 - m'_2) \quad (5)$$

From eqn. 5 and noting that both sides must have same sign, we find that  $(m_1 - m'_1)$  and  $(m_2 - m'_2)$  are both positive or negative. Assuming that both  $m_1 - m'_1$  and  $m_2 - m'_2$  are positive integers, then

$$a_{11}(m_1 - m'_1) + a_{12}(m_2 - m'_2) > a_{11} + a_{12} \quad (6)$$

From eqn. 2 the left-hand side of eqn. 6 is  $m - m'$ , and thus the condition on the magnitude of  $m - m'$  is violated. A similar condition can be obtained when both  $m_1 - m'_1$  and  $m_2 - m'_2$  are negative. Hence  $m_e \neq m'_e$ .

**Decryption:** To decrypt the cryptogram, the following steps are needed:

- (1) Compute  $m_{ei} = m_e \pmod{p_i}, i = 1, 2$ .
- (2) Solve the following pair of linear simultaneous equations in two unknowns  $t_1$  and  $t_2$  (which are rational numbers):

$$\begin{aligned} a_{11}t_1 + a_{12}t_2 &= m_{e1} \\ a_{21}t_1 + a_{22}t_2 &= m_{e2} \end{aligned} \quad (7)$$

(3) Form

$$\begin{aligned} k_1 &= \lfloor t_1 \rfloor \\ k_2 &= \lfloor t_2 \rfloor \end{aligned}$$

(4) Compute

$$a_{i1}k_1 + a_{i2}k_2 = m'_{ei} \quad i = 1, 2$$

(5) Form  $m_{ei} - m'_{ei} = m$

To justify the decryption algorithm, we observe that

$$t_i = [t_i] + \gamma_i/\Delta \quad i = 1, 2$$

where

$$\Delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

and  $\gamma_i/\Delta$  is the proper fraction.

Rewrite eqn. 7 as

$$\begin{aligned} a_{11}t_1 + a_{12}t_2 &= x_1 + m \\ a_{21}t_1 + a_{22}t_2 &= x_2 + m \\ t_1 &= (a_{22}x_1 - a_{12}x_2)/\Delta + m(a_{22} - a_{12})/\Delta \\ t_2 &= (a_{21}x_1 - a_{11}x_2)/-\Delta + m(a_{21} - a_{11})/-\Delta \end{aligned} \quad (8)$$

But, from eqn. 3,

$$\begin{aligned} m_1\Delta &= a_{22}x_1 - a_{12}x_2 \\ m_2\Delta &= -a_{21}x_1 + a_{11}x_2 \end{aligned} \quad (9)$$

Hence, from eqns. 3, 8 and 9, we have

$$\begin{aligned} t_1 &= m_1 + m(a_{22} - a_{12})/\Delta \\ t_2 &= m_2 + m(a_{21} - a_{11})/-\Delta \end{aligned}$$

That  $m(a_{22} - a_{12})/\Delta$  and  $m(a_{21} - a_{11})/-\Delta$  are proper fractions can be verified using eqns. 1 and 2. Therefore the decomposition above is unique.

Thus

$$[t_1] = m_1 \quad [t_2] = m_2$$

Hence in decryption step 4 the computed values are actually  $x_i$ , as given in eqn. 3. Step 5 is therefore justified.

**Conclusions:** The data expansion due to encryption is around 1:2.5 and is therefore moderate. The public key is about 1.5 kbit long, and the storage requirement is therefore quite low when compared to other knapsack-like public key cryptosystems. Finally, the scheme appears to be resistant to the cryptanalytic attacks on the original Lu-Lee scheme.

B. S. ADIGA

14th June 1985

Systems Engineering Division  
National Aeronautical Laboratory  
Bangalore 17, India

P. SHANKAR

School of Automation  
Indian Institute of Science  
Bangalore 12, India

## References

- 1 LU, S. C., and LEE, L. N.: 'A simple and effective public-key cryptosystem', *COMSAT Tech. Rev.*, 1979, 9, pp. 15-24
- 2 ADLEMAN, L. M., and RIVEST, R. L.: 'How to break the Lu-Lee (COMSAT) public-key cryptosystem'. MIT Laboratory for Computer Science, July 1979
- 3 KOCHANSKI, M. J.: 'Remarks on Lu and Lee's proposals', *Cryptologia*, 1980
- 4 GOETHALS, J. M., and COUVREUR, C.: 'A cryptanalytic attack on the Lu-Lee public-key cryptosystem', *Philips J. Res.*, 1980, 35, pp. 301-306

## NEW FABRICATION TECHNIQUE FOR SINGLE-PHASE UNIDIRECTIONAL SAW FILTER (EMUDT) IN UHF RANGE

**Indexing terms:** Ultrasonics, Surface-acoustic-wave devices, Directional couplers, Transducers

New fabrication techniques for single-phase unidirectional SAW filters (EMUDT) utilising the self-aligned angle-evaporation technique are described. The experimental results show a directivity of 10.0 dB/transducer at 483 MHz.

**Introduction:** A surface-acoustic-wave (SAW) filter employing the conventional interdigital transducer (IDT) shows an inherent minimum insertion loss of 6 dB, because of bidirectionality and strong passband ripple due to triple-transit echo and secondary effects. To avoid these flaws, the three-transducer arrangement has been proposed. The unidirectional transducer, however, represents a much more advantageous method of overcoming the above-mentioned defects, and, among others, the following suggestions have already been made: (i) 3-phase unidirectional transducer,<sup>1</sup> (ii) group type of unidirectional transducer with  $\lambda_0/4$ -phase shifter,<sup>2</sup> and (iii) single-phase unidirectional transducer (SPUDT) using internal reflection,<sup>3</sup> a reflection bank,<sup>4</sup> reflection due to the change of the electromechanical coupling coefficient (EMUDT)<sup>5</sup> and floating electrode reflection.<sup>6</sup>

In this letter we describe a new fabrication technique for a new EMUDT utilising self-aligned angle evaporation. The techniques use only one photomask and no mask alignment for the interdigital fingers of EMUDT.

**Description of new EMUDT:** The basic arrangement of the new EMUDT is shown schematically in Fig. 1. Some parts of electrodes (Al) are fabricated direct on  $128^\circ$  y-x LiNbO<sub>3</sub>, while other parts of the electrodes are fabricated on the strips of the very thin dielectric film (SiO<sub>2</sub>). The electromechanical coupling coefficient ( $K^2$ ) of the electrodes on SiO<sub>2</sub> strips is less than that of the electrodes on LiNbO<sub>3</sub>. Furthermore, the SiO<sub>2</sub>

strips operate as the reflector, owing to the mass loading effects. The reflection coefficient of the new EMUDT is larger. We can thus obtain a larger directivity than for the older one.<sup>5</sup>

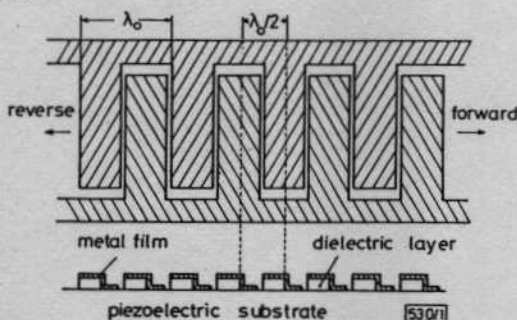


Fig. 1 Configuration of new EMUDT with strips of very thin dielectric film (SiO<sub>2</sub>)

The analysis of the device is performed using the equivalent circuit model. The IDT is divided in four sections per half-wavelength. The transfer ratios of the equivalent circuit model are varied to correspond to the value of  $K^2$ . In addition, the reflection effects due to mass loading of the thin SiO<sub>2</sub> strips are taken into account.

Calculated results for new EMUDT are shown in Fig. 2, where the number of pairs of electrode is 30 and the thickness ratio of SiO<sub>2</sub> ( $H/\lambda_0$ ) is 0.02 ( $H$  is the thickness of the dielectric film and  $\lambda_0$  is the SAW wavelength). The minimum insertion loss is about 1.0 dB and the bandwidth is about 3% for sending and receiving transducers.

**Experimental results:** To verify these principles, a few sample patterns have been fabricated on  $128^\circ$  y-x LiNbO<sub>3</sub>. The design details are as follows: a three-transducer system is employed, the centre transducer being a unidirectional EMUDT with a pair number of 30 and a film thickness of  $0.24 \mu\text{m}$  ( $H/\lambda_0 = 0.02$ ), and the other two being conventional IDTs with pair numbers of 4.